1. Let’s discuss the protocol RSA that uses the Asymmetric key.
2. **RSA**: This is the single protocol in modern network and certificate communications.
3. Jatin: Just take a look at the below image.A diagram of a algorithm

   Description automatically generated
4. **RSA** was abbreviated after the three developers of the Public Key Cryptosystem.  
   R: Rivest.  
   S: Shamir.  
   A: Adleman.
5. RSA is not just a protocol rather it is **Public-Key Cryptosystem** using which we can create new keys Private and Public.
   1. We can create keys of different length.
   2. Actually, the following is the applications of RSA for different purpose that RSA supports.
      1. **Secure Data Transmission**: We can encrypt and decrypt.
      2. **Authenticity of sender and Integrity of Data**: We can check the authenticity and integrity of sender and data respectively.
         1. Authenticity: If we are able to decrypt encrypted (data or hashcode) with corresponding public key.
         2. Integrity: If the hashcode received and generated both matches.
      3. Jatin: **Securely Exchange Symmetric Key**: Used to exchange a symmetric encryption key.
6. When generating keys, both public and private are created in pairs not individually. So, their length is always same.
7. If private key is compromised, please create a new key pair and   
   if we need to create certificate based on that pair, please recreate certificate as well.
8. A close-up of a number

   Description automatically generated
9. 